UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/757,963	01/10/2001	John S. Flowers	HVWD-01008US0 MEM/SBS	9385

758 7590 10/31/2003

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	15

DATE MAILED: 10/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/757,963	FLOWERS ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-40* is/are pending in the application.

4a) Of the above claim(s) *14,26 and 38* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-13, 15-25, 27-37, 39, 40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 5-40 are pending in the application.

2. Claims 5-11, 17-23 and 29-35 have been amended.

3. Claims 14, 26, and 38 have been cancelled.

Response to Amendment

4. The examiner withdraws 35 USC § 101 for claims 5-28. With the amendment, the applicant has overcome the rejection.

5. By canceling claims 14, 26, and 38, the applicant has overcome 35 USC § 112(1) claim rejection.

6. The examiner withdraws 35 USC § 112(2) for claim 40. With the amendment, the applicant has overcome the rejection.

Response to Arguments

7. Applicant's arguments with respect to claims 5-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002

do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 5-8, 12, 13, 17-20, 24, 25, 29-32, 36 and 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Huff et al U.S. Patent No. 6,415,321 B1.

As to claims 5, 17 and 29 Huff et al discloses a vulnerability detection system (VDS) for gathering information about the network to determine vulnerabilities of a plurality of hosts on the network [column 3, lines 18-29]. Huff et al discloses an intrusion detection system (IDS) for examining network traffic responsive to the vulnerabilities of a host from the plurality of hosts as determined by the VDS to detect traffic indicative of malicious activity [column 10 line 54 to column 11 line 6].

As to claims 6, 18 and 30, Huff et al discloses that the VDS is adapted to gather information about the network by sending data to the plurality of hosts and receiving responsive data from the plurality of hosts [column 3, lines 12-29].

As to claims 7, 19 and 31, Huff et al suggests that the VDS is adapted to gather information automatically provided by the plurality of hosts [column 9, lines 6-17].

As to claims 8, 20 and 32, Huff et al discloses a vulnerabilities rules database, in communication with the VDS, for storing rules describing vulnerabilities of the plurality of hosts [column 7, lines 52-65]. Huff et al discloses that the VDS is adapted to analyze the gathered information with the rules to determine the vulnerabilities of the plurality of hosts [column 8, lines 35-56].

As to claims 12, 24 and 36, Huff et al discloses an intrusion rules database in communication with the IDS, for storing rules describing malicious activity [column 10 line 54 to column 11 line 6]. Huff et al discloses that the IDS is adapted to analyze the network traffic with the rules to detect network traffic indicative of exploitations of the determined vulnerabilities [column 10 line 54 to column 11 line 6].

As to claims 13, 25 and 37, Huff et al suggests that the IDS is adapted to detect traffic indicative of exploitations of only the determined vulnerabilities [column 7, lines 52-65].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 9-11, 21-23 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huff et al U.S. Patent No. 6,415,321 B1 as applied to claims 5, 17 and 29 above, and further in view of Gleichauf et al U.S. Patent No. 6,415,321 B1.

As to claims 9-11, 21-23 and 33-35, Huff et al does not teach that the VDS is adapted to analyze the gathered information with the rules to identify operating systems on the plurality of hosts and determine the vulnerabilities responsive to the respective operating systems. Huff et al does not teach that the VDS is adapted to analyze the gathered information with the rules to identify open ports on the plurality of hosts and determine the vulnerabilities based on the open ports. Huff et al does not teach that the VDS is adapted to analyze the gathered information with

the rules to identify applications executing on the plurality of hosts and determine the vulnerabilities based on the applications.

Gleichauf et al teaches that the VDS is adapted to analyze the gathered information with the rules to identify operating systems on the plurality of hosts and determine the vulnerabilities responsive to the respective operating systems [column 5, lines 15-31]. Gleichauf et al teaches that the VDS is adapted to analyze the gathered information with the rules to identify open ports on the plurality of hosts and determine the vulnerabilities based on the open ports [column 5, lines 15-31]. Gleichauf teaches that the VDS is adapted to analyze the gathered information with the rules to identify applications executing on the plurality of hosts and determine the vulnerabilities based on the applications [column 6, lines 48-65].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Huff et al so the VDS would have been able to analyze the gathered information to identify operating systems, open ports, and applications on the plurality of hosts to determine the vulnerabilities based on the operating systems, open ports, and applications.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Huff et al by the teaching of Gleichauf et al because the examiner asserts that certain operating systems and applications running on a computer are more open to attacks. The examiner asserts that open ports make a computer more vulnerable to attacks.

10. Claims 15, 16, 27, 28, 39 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huff et al U.S. Patent No. 6,415,321 B1 as applied to claims 5, 17 and 29 above, and further in view of examiner's official notice.

As to claims 15, 16, 27, 28, 39 and 40, Huff et al does not teach that the VDS is adapted to update the determined vulnerabilities and that the IDS is adapted to detect traffic indicative of malicious activity in response to the update. Huff et al does not teach that the VDS is adapted to update the determined vulnerabilities in response to a change in the network.

The examiner takes official notice that new network devices are added to a network and that new network devices introduce new vulnerabilities.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Huff et al so that the new vulnerabilities would have been updated and that the IDS would have detected traffic indicative of malicious traffic with respect to the updated vulnerabilities. New vulnerabilities would have been detected if new devices are introduced on the network and the IDS would have detected traffic indicative of malicious traffic with respect to the updated vulnerabilities.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Huff et al because one would have been able to protect the network from new exploitations and malicious traffic when new network devices and vulnerabilities are introduced.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy
October 28, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100